

AMENDMENT OF THE CLAIMS

WHAT IS CLAIMED IS:

1. (Currently amended) A method for e-commerce with a check, the method comprising:
providing a purchaser with an encoded personal identification number (PIN), wherein the
PIN is generated when the purchaser makes an offer of payment, wherein further
the PIN enables the purchaser to make an electronic transaction of web commerce
over the Internet;
receiving the encoded PIN in response to the offer of payment by the purchaser to a
merchant with [[a]] the check, by a bank associated with the check, wherein the
bank is to decode the encoded PIN;
decoding the encoded PIN; [[and]]
comparing the decoded PIN with information associated with the purchaser to
authenticate the purchaser and to verify that sufficient funds are available to the
purchaser for the electronic transaction; and
enabling immediate clearance of the check based on the comparing and the verification of
sufficient funds.
2. (Original) The method of claim 1, wherein providing the purchaser with the encoded
PIN comprises providing the purchaser with software to generate the encoded PIN,
wherein generating the encoded PIN comprises encrypting a PIN.
3. (Original) The method of claim 1, wherein providing the purchaser with the encoded
PIN comprises interacting with the purchaser to generate the encoded PIN prior to the
transaction.
4. (Original) The method of claim 1, wherein receiving the encoded PIN comprises
receiving the encoded PIN, forwarded by the merchant to the bank, in an encrypted form
such that the merchant is a conduit through which the purchaser transmits to the encoded
PIN to the bank.

5. (Currently amended) The method of claim 1, wherein receiving the encoded PIN comprises receiving [[the]] transaction information with the encoded PIN, wherein the transaction information comprises a routing number, a bank account number, a check number, and an amount associated with the transaction.
6. (Currently amended) The method of claim 1, wherein decoding the encoded PIN comprises decrypting the encoded PIN to determine the date and time of the generation of the encoded PIN.
7. (Original) The method of claim 6, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN based upon a unique transaction number associated with the purchaser.
8. (Original) The method of claim 6, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN based upon an amount associated with the transaction.
9. (Original) The method of claim 6, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN based upon a date associated with the transaction.
10. (Original) The method of claim 1, wherein comparing the decoded PIN comprises comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction.
11. (Currently amended) An apparatus for e-commerce with a check, the apparatus comprising:
a PIN module to provide a purchaser with an encoded personal identification number (PIN), wherein the PIN is generated when the purchaser makes an offer of payment, wherein further the offer of payment is for an electronic transaction of web commerce over the Internet;

- a purchaser database to maintain information associated with the purchaser and an account associated with the purchaser; and
- a PIN processor to receive the encoded PIN in response to the offer of payment by the purchaser to a merchant with a check, decode the encoded PIN, and compare the decoded PIN with the information associated with the purchaser to ~~authenticate~~ verify the identity of the purchaser and to verify that sufficient funds are available to the purchaser for the electronic transaction.
12. (Currently amended) The apparatus of claim 11, wherein the PIN module comprises a client-side software application ~~configured~~ programmed to generate the encoded PIN, the client-side software being configured to independently determine a unique transaction identification that authenticates the purchaser for the transaction to a bank associated with the account, wherein further the PIN module is programmed to transmit the encoded PIN directly to a bank of the purchaser.
13. (Currently amended) The apparatus of claim 11, wherein the PIN module comprises a software application configured to interact with a purchaser to encrypt a password to generate the encoded PIN, wherein further the PIN module comprises a shopping cart plug-in.
14. (Currently amended) The apparatus of claim 11, wherein the PIN processor is ~~configured~~ programmed to receive the encoded PIN from the merchant and to enable immediate clearance of the check based upon the comparison of the decoded PIN and the verification of sufficient funds, wherein the encoded PIN is designed to prevent the merchant from accessing identification information of the encoded PIN.
15. (Original) The apparatus of claim 11, wherein the PIN processor comprises a PIN decrypter to decrypt the encoded PIN.
16. (Currently amended) The apparatus of claim 15, wherein the PIN processor further comprises a PIN decoder to decode the decrypted, encoded PIN, wherein further the PIN

decoder is arranged to decode PINs encoded by different account holders by utilizing information associated with the corresponding accounts.

17. (Original) The apparatus of claim 11, wherein the PIN processor comprises a comparator to compare the transaction amount with funds available to the purchaser for the transaction.
18. (Currently amended) The apparatus of claim 17, wherein the comparator is ~~configured~~ programmed to compare a password embedded in the decoded PIN against a password received from the purchaser for the transaction.
19. (Currently amended) A machine-accessible medium containing instructions, which when executed by a machine, cause said machine to perform operations, comprising:
providing a purchaser with an encoded personal identification number (PIN), wherein the PIN is generated when the purchaser makes an offer of payment, wherein further the offer of payment is for an electronic transaction of web commerce over the Internet;
receiving the encoded PIN in response to the offer of payment by the purchaser to a merchant with a check, by a bank associated with the check, wherein the bank is to decode the encoded PIN;
decoding the encoded PIN; and
comparing the decoded PIN with information associated with the purchaser to authenticate the purchaser and to verify that sufficient funds are available to the purchaser for the transaction.
20. (Currently amended) The machine-accessible medium of claim 19, further comprising transmitting an indication that funds will be transferred to a merchant bank, wherein providing the purchaser with the encoded PIN comprises providing the purchaser with software to generate the encoded PIN.
21. (Currently amended) The machine-accessible medium of claim 19, further comprising authorizing the electronic transaction and transmitting approval to the merchant, wherein

providing the purchaser with the encoded PIN comprises interacting with the purchaser to encrypt a PIN to generate the encoded PIN prior to the transaction.

22. (Original) The machine-accessible medium of claim 19, wherein decoding the encoded PIN comprises decrypting the encoded PIN.
23. (Original) The machine-accessible medium of claim 22, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN.
24. (Original) The machine-accessible medium of claim 19, wherein comparing the decoded PIN comprises comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction.
25. (Currently amended) A machine-accessible medium containing instructions, which when executed by a machine, cause said machine to perform operations, comprising:
providing a person with an encoded personal identification number (PIN), wherein the PIN is generated via interaction of the person based on facts of an offer of payment, wherein further the interaction is for an electronic transaction of web commerce over the Internet between the person and a merchant;
receiving the encoded PIN in response to the offer of payment by the person to [[a]] the merchant with a check, by a bank associated with the check, wherein the bank is to decode the encoded PIN;
decoding the encoded PIN; and
comparing the decoded PIN with information associated with the person to authenticate the person.
26. (Currently amended) The machine-accessible medium of claim 25, further comprising encrypting the encoded PIN and immediately transferring funds for the offer of payment based on the comparing the decoded PIN.
27. (Currently amended) The machine-accessible medium of claim 25, further comprising enabling the person to log into a PIN module to generate the encoded PIN, further

comprising comparing a transaction amount with funds available to the person for the offer of payment to verify that sufficient funds are available to the person.

28. (Previously presented) The machine-accessible medium of claim 25, further comprising comparing a password embedded in the decoded PIN against a password received from the person.
29. (Currently amended) The machine-accessible medium of claim 25, wherein the providing the person with an encoded PIN comprises using the facts of the offer of payment to encode the PIN, wherein further one of the facts comprises ~~one of a date, a time, an expiration time, a password, an account number, a check number, a routing number, and an amount of money.~~
30. (Currently amended) The machine-accessible medium of claim 25, wherein the providing the person with an encoded PIN comprises using a client-side software application configured to generate the encoded PIN, the client-side software being ~~configured~~ programmed to independently determine a unique transaction identification that authenticates the person for the transaction to a bank associated with the account.